WHAT IS CLAIMED IS:

1. A sequence generator including:

a plurality of linear feedback shift registers operable to generate a plurality of binary sequences,

a plurality of nonlinear functions having said binary sequences as their input and operable to generate a second plurality of binary sequences,

at least first and second switches,

a controller including a shift register operable to control said first and second switches,

the first switch operative to select one of said second plurality of binary sequences to the first bit of the shift register, and the second switch operative to select one of said second plurality of binary sequences to an output.

2. A sequence generator for generating a pseudo random sequence for random number generation or a stream cipher engine including:

a sequence generator operable to generate a first plurality of binary sequences,

at least first and second nonlinear function generators having said first plurality binary sequences as their input, the first generator operative to generate a second plurality of binary sequences and the second generator operative to generate a third plurality of binary sequences,

at least first and second switches,

a controller having an input and at least first and second outputs operable to control said first and second switches,

the first switch operable to select one said second plurality of binary sequences to the input of the controller, and the second switch operable to select one of said third plurality of binary sequences to an output.

3. A sequence generator according to claim 2 wherein the sequence generator includes a plurality of feedback shift registers each operable to generate a binary sequence.

4. A sequence generator according to claim 2 wherein the nonlinear function generators includes a plurality of boolean functions, each boolean function having the first plurality of binary sequences as an input and being operable to generate a binary sequence.

5. A sequence generator according to claim 2 wherein the switches are multiplexers.

6. A sequence generator according to claim 2 wherein the controller includes a shift register, the input of the controller being the first bit of the register and the outputs of the controller being at positions along the register.

7. A method of generating a pseudo random sequence for random number generation or a stream cipher engine including generating a first plurality of binary sequences, applying a plurality of nonlinear functions to said first plurality of binary sequences to obtain an uncorrelated second plurality of binary sequences, and randomly selecting an output sequence from one of the second plurality of binary sequences.

8. A method according to claim 7 wherein the nonlinear functions are arranged to provide a one-to-many relationship between the first and second plurality of binary sequences.

9. A method according to claim 7 wherein the nonlinear functions are boolean functions.

10. A method according to claim 7 wherein the output sequence is randomly selected by applying one of the second plurality of binary sequences to a shift register.